UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,179	12/02/2003	Simon Robert Walmsley	PEA16US	5306

24011   7590   03/05/2008
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER
HOANG, DANIEL L

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
03/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/727,179	WALMSLEY ET AL.
	Examiner	Art Unit	
	DANIEL L. HOANG	2136	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>24 September 2007</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-10</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-10</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
          application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see page 1, filed 9/24/07, with respect to the rejection(s) of claim(s) 1 under 35

USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of Silverbrook, US

Patent No 6,745,331.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-8, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Hameau et al., US PGP No. 20020107798 and further in view of Silverbrook et al, US
Patent No. 6246970 and Silverbrook, US Patent No. 6,745,331.

As per claim 1:

Hameau teaches:

An integrated circuit comprising a processor and non-volatile memory, the non-volatile memory storing a

first number and a second number, wherein the second number is the result of an encryption function

taking a third number and secret information as operands, the integrated circuit comprising software

configured to decrypt the second number using the first number, thereby to determine the secret

information as required.

> *[see paragraph 8] "Written into a nonvolatile part of the aforementioned storage means of the
> microchip, in permanent (using "Read Only Memory" or "ROM"), or semi-permanent ("Electrically*

> *Erasable Programmable Read Only Memory" or "EEPROM") fashion, is so-called secret data required for these functions: encryption algorithm, secret encryption keys, identification data, etc."*
>
> *[see paragraph 50] "As shown in FIG. 2, using an outgoing order O.sub.s, the "SAM" 3 retrieves from the smart card CP a sixteen-byte random number N.sub.aC. The number N.sub.aC will hereinafter be called the "card random number," and can be generated, for example, by the computing means of the smart card CP, in the example illustrated a microprocessor CPU. The "SAM" 3 also generates a sixteen-byte random number that will be called the "SAM random number" N.sub.aS."*
>
> *[see paragraph 58] "From the secret master key K.sub.M and from the aforementioned sixteen-byte random number N.sub.aC, the smart card CP generates a sixteen-byte symmetric, secret so-called session key K.sub.S, making it possible to calculate a cryptogram specific to the smart card CP."*
>
> *[see paragraph 66] "The "SAM" 3 is capable of calculating the same secret session key K.sub.S in the manner just described, since the latter also stores the secret master key K.sub.M."*

As is evident in the citations above, the smart card comprising a microchip is interpreted as the claimed "integrated circuit comprising a memory." As is also cited, the nonvolatile part of the smart card stores secret data. The master key of the smart card is being interpreted as the claimed "first number". The master key of the SAM is being interpreted as the claimed "third number". The sixteen byte random number is being interpreted as the claimed "secret information". The secret session key that is generated using the secret master key and the sixteen byte random number is interpreted as the claimed "second number". As is consistent with the claim, the secret session key is the result of an encryption function taking the master key and the sixteen byte random number as the operands. As can be seen in paragraphs 25 and 26 of the reference, the smart card can derive the secret information sent from the SAM by using its own copy of the master key.

Hameau does not teach:

Arranging a tamper detection line to obscure the operation of non-volatile memory.

Silverbrook et al teaches:

[see col. 4, lines 39-49]

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Hameau reference to include usage of a tamper detection line in order to detect possible attacks.

The above combination does not teach:

The tamper detection line being arranged to pass directly over reach data bit of the non-volatile memory so as to obscure operation of the non-volatile memory.

Silverbrook teaches:

[see col. 68, lines 46-59]

It would have been obvious to one of ordinary skill in the art to modify the above combination to include the above limitation to "ensure that an attacker cannot probe the contents" of the non-volatile memory.

As per claim 2, Hameau teaches:

An integrated circuit according to claim 1, wherein the first and third numbers are the same.

> [see paragraph 23] "storage means of said microchip storing a *symmetric secret encryption key* and an asymmetric public key and said security device storing the *same symmetric secret encryption key*."

As per claim 3, Hameau teaches:

An integrated circuit according to claim 1, wherein the first and second numbers are of the same length.

> [see rejection of claim 2, wherein both are the same and thus clearly are the same length.]

As per claim 5, Hameau teaches:

An integrated circuit according to claim 1, wherein the encryption function is an XOR logical function.

> [see paragraph 63] "The part K.sub.S1 is re-injected through a first input of a logic circuit of the "exclusive-OR" type, referenced XOR."

As per claim 6, Hameau teaches:

An integrated circuit according to claim 5, wherein the software is configured to decrypt the second

number by performing an XOR logical function using the first and second numbers as operands.

> *[see paragraph 65] "the "exclusive-OR" logic operation can be performed by means of software
> instead of using a specific logic circuit XOR, by calling a routine stored in "ROM" memory 1, for
> example, under the control of the microprocessor CPU."*

As per claim 7, Hameau teaches:

A method of manufacturing a plurality of integrated circuits in accordance with claim 1, including the

steps, for each integrated circuit, of: determining the first number, the third number and the secret

information; generating the second number by way of an encryption function that uses the third number

and the secret information as operands; storing the first and second numbers on the integrated circuit.

> *[see paragraph 80] "The method makes it possible to load, into each smart card CP, its own key,
> or in other words a different key than the other smart cards.*

As per claim 8, Hameau teaches:

A method according to claim 7, wherein the first number is different amongst at least a plurality of the

integrated circuits.

> *[see rejection of claim 7 wherein each smart card is loaded with its own keys]*

As per claim 10, Hameau teaches:

A method according to claim 7, wherein the first number is stored on the integrated circuit first, then

extracted therefrom for use in generating the third and thence the second number.

> *[see rejection of claim 1, wherein the master key is stored on the smart card and then used to*
>
> *derive the remaining security data]*

Claims 4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Hameau as applied to claim 1 above, and further in view of Pires (US Patent No.

6,269,164.

As per claim 4:

An integrated number according to claim 1, wherein the first number is a random number that was
generated using a stochastic process.

> *The Hameau reference has been discussed above. Hameau does not expressly disclose that the*
>
> *first number is a random number that is generated using a stochastic process. Pres teaches of a*
>
> *stochastic key.*
>
> *[see col. 18, lines 2-7] "stochastic key scrambling method previously described is particularly well*
>
> *suited to the creation of good keys. As stated before, a good key is one made by a process that*
>
> *distributes the keys it generates evenly over the entirety of the available key space regardless of*
>
> *the input used to create it."*

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the

subject matter pertains to modify the Hameau reference to incorporate the teachings of Pires in order to

include usage of a random key generated using a stochastic process in order to improve upon the

security of the key and to generate a key that is difficult to obtain because it is created through a random

process.

As per claim 9, Hameau teaches:

A method according to claim 8, wherein the first numbers are determined randomly, pseudo-randomly, *or*
arbitrarily.

> *[see rejection of claim4 wherein a stochastic process leads to randomness]*

CONCLUSION

*.   Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

> Commissioner for Patents
> P.O. Box 1450
> Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

> Customer Service Window
> Randolph Building
> 401 Dulaney Street
> Alexandria, VA 22314

*.   Any inquiry concerning this communication or earlier communications from the examiner should

be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally

be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where

this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be obtained from

either Private PAIR or Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)

at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2136
2/25/08

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136